Math 192r, Problem Set #5: Solutions

1. *There is a unique polynomial of degree d such that $f(k) = 2^k$ for $k = 0, 1, ..., d$. What is $f(d+1)$? What is $f(-1)$?*

   Suppose $g(k)$ is a polynomial of degree $m \geq 1$, so that its sequence of mth differences is constant. If we define $G(k) = g(k) + g(k-1) + \ldots + g(1)$ for all $k \geq 1$, then the first differences of G are the "zeroeth" differences of g, the second differences of G are the first differences of g, and so on, so that the sequence of $m+1$st difference of G is constant, implying that $G(k)$ is given by a polynomial of degree $m+1$ in k. This last assertion is true for $g(k-1)+g(k-2)+\ldots+g(0)+1$ as well, since it differs from $G(k)$ by the substitution of $k-1$ for k and the addition of the constant 1.

   In particular, we see that if f is a polynomial of degree $d-1$ with $f(k) = 2^k$ for $0 \leq k \leq d-1$, then the sum $F(k) = f(k-1) + f(k-2) + \ldots + f(0) + 1$ defines a polynomial function of degree d, and it is easy to see that if f satisfies the property that characterizes f_{d-1}, F satisfies the property that characterizes f_d. Hence we have

   $$f_d(k) = f_{d-1}(k-1) + f_{d-1}(k-2) + \ldots + f_{d-1}(0) + 1$$

   for all $k \geq 0$ (not just $0 \leq k \leq d$), with the proviso that in the case $k = 0$, the only term on the right hand side is the 1.

   Putting $k = d+1$, we have $f_d(d+1) = f_{d-1}(d) + f_{d-1}(d-1) + \ldots + f_{d-1}(0) + 1 = f_{d-1}(d) + 2^{d-1} + \ldots + 1 + 1 = f^{d-1}(d) + 2^d$. That is, the sequence $f_0(1), f_1(2), f_2(3), \ldots,$ has the sequence $1, 2, 4, \ldots$ as its sequence of first differences, from which it follows (say by induction) that $f_{d-1}(d) = 2^d - 1$.

   On the other hand, for each fixed d the relation $f_d(k) - f_d(k-1) = f_{d-1}(k-1)$ holds for all k, since it holds for all positive k and since both sides of the equation are polynomials. Hence we have $f_d(0) - f_d(-1) = f_{d-1}(-1)$. Rewriting this as $f_d(-1) = f_d(0) - f_{d-1}(-1)$ and using the fact that $f_d(0) = 1$, we have $f_d(-1) = 1 - f_{d-1}(-1)$, from which it follows (say by induction) that $f_d(-1) = (-1)^d$.

   Note that you don't need to have an explicit formula for $f_d(k)$ in order to solve this problem!

2. *One basis for the space of polynomials of degree less than d is the monomial basis $1, t, t^2, ..., t^{d-1}$. Another is the shifted monomial basis $1, (t+1), (t+1)^2, ..., (t+1)^{d-1}$. Call these bases $u_1, ..., u_d$ and $v_1, ..., v_d$ respectively.*

   (a) *Derive a formula for the entries of the change-of-basis matrix M expressing the u_i's as linear combinations of the v_j's.*

   We seek a d-by-d matrix M that, when multiplied on the right by the column vector e_i (with a 1 in the ith position and a 0 everywhere else), gives a column vector $(c_1, c_2, \ldots, c_d)^T$ such that $u_i = c_1 v_1 + c_2 v_2 + \ldots + c_d v_d$. Now $u_i = t^{i-1} = ((t+1) - 1)^{i-1} = \sum_{j=0}^{i-1} \binom{i-1}{j} (t+1)^j (-1)^{i-1-j} = \sum_{j=0}^{i-1} \binom{i-1}{j} v_{j+1} (-1)^{i-1-j} = \sum_{j=1}^{i} \binom{i-1}{j-1} v_j (-1)^{i-j}$, so $c_j = (-1)^{i-j} \binom{i-1}{j-1}$ (which gets interpreted as 0 for $j > i$). Hence

$$M_{j,i} = \begin{cases} (-1)^{i-j}\binom{i-1}{j-1} & \text{for } 1 \le j \le i \le n, \\ 0 & \text{otherwise.} \end{cases}$$

   (Note: I didn't specify whether the vectors were to be treated as row-vectors or column-vectors, or equivalently, whether the change-of-basis matrix was supposed to be applied on the right or on the left. If you adopted the row-vector approach, you would find that the answers you got for parts (a) and (b) are reversed, relative to mine.)

   (b) *Derive a formula for the entries of the change-of-basis matrix N expressing the v_j's as linear combinations of the u_i's.*

   This one is even easier: $v_j = (t+1)^{j-1} = \sum_{i=0}^{j-1} \binom{j-1}{i} t^i = \sum_{i=1}^{j} \binom{j-1}{i-1} u_i$ so

$$N_{i,j} = \begin{cases} \binom{j-1}{i-1} & \text{for } 1 \le i \le j \le n, \\ 0 & \text{otherwise.} \end{cases}$$

   (c) *From the description of M and N as basis-change matrices, we know that $MN = NM = I$. Forgetting for the moment what M and N mean, rewrite the assertions $MN = NM = I$ as binomial coefficient identities, and prove them either algebraically or bijectively.*

The assertion $MN = I$ can be rewritten as $\sum_j M_{i,j}N_{j,k} = \delta_{i,k}$, where $\delta_{i,j}$ is 1 if $i = j$ and 0 otherwise. That is, $\sum(-1)^{j-i}\binom{j-1}{i-1}\binom{k-1}{j-1} = \delta(i,k)$ where the sum is over all j such that $i \leq j \leq k$. For convenience, we shift indices and write this as

$$\sum(-1)^{j-i}\binom{j}{i}\binom{k}{j} = \delta(i,k)$$

where the sum is still over all j such that $i \leq j \leq k$.

Algebraic proof: The sum in question is the coefficient of x^{k-i} in the product of $\binom{i}{i} - \binom{i+1}{i}x + \binom{i+2}{i}x^2 - \ldots + (-1)^{k-i}\binom{k}{i}x^{k-i} + \ldots$ and $\binom{k}{k} + \binom{k}{k-1}x + \binom{k}{k-2}x^2 + \ldots + \binom{k}{i}x^{k-i} + \ldots + \binom{k}{0}x^k$. The first factor can be recognized as $(1+x)^{-(i+1)}$ (by the binomial theorem) and the latter can be recognized as $(1+x)^k$. So the product is $(1+x)^{k-i-1}$. The coefficient of x^{k-i} in the formal power series expansion of $(1+x)^{k-i-1}$ is 0 as long as $k-i-1$ is non-negative, since in that case $(1+x)^{k-i-1}$ is just a polynomial of degree less than $k-i$. However, when $i = k$, $(1+x)^{k-i-1}$ becomes the formal power series $(1+x)^{-1} = 1-x+x^2-x^3+\ldots$, in which the coefficient of x^{k-i} is just the constant term 1.

Combinatorial proof: Given a set C of size k, $\sum(-1)^{j-i}\binom{j}{i}\binom{k}{j}$ counts the number of ways to choose a subset $B \subset C$ of size j and a subset $A \subset B$ of size i, where a choice of A, B, C counts as positive or negative according to whether the number of elements of B that are not in C is even or odd. If we hold the subset A fixed and do a signed enumeration of the sets B satisfying $A \subset B \subset C$, we find that the signed count is 1 if $A = C$ and 0 otherwise. (Reason: This is just like signed enumeration of the subsets of $C \setminus A$, where a set counts as positive or negative according to whether it has an even or odd number of elements.) If $i = k$, there is exactly one set A, namely C itself, whose aggregate contribution is non-zero, and in this case the aggregate contribution is 1; whereas if $i < k$, all the aggregate contributions vanish. This proves the identity.

The assertion $NM = I$ can be rewritten as $\sum_j N_{i,j}M_{j,k} = \delta_{i,k}$, that is, $\binom{j-1}{i-1}(-1)^{k-j}\binom{k-1}{j-1} = \delta_{i,j}$. Re-indexing, we write $(-1)^{k-j}\binom{j}{i}\binom{k}{j} = \delta_{i,j}$. The proofs are similar to what appeared above.